tranSMART

User Administration Guide

September 16, 2013, Version 1.1

Contents

Chapter 1

User Administration Overview

As tranSMART User Administrator, you are responsible for the following tasks:

- Adding new users to the tranSMART access list
- Granting permissions to users through role assignments and access rights to private Dataset Explorer studies
- Creating user groups, and assigning these groups access rights to private Dataset Explorer studies
- Creating and mapping user roles
- Setting up security for private Dataset Explorer studies

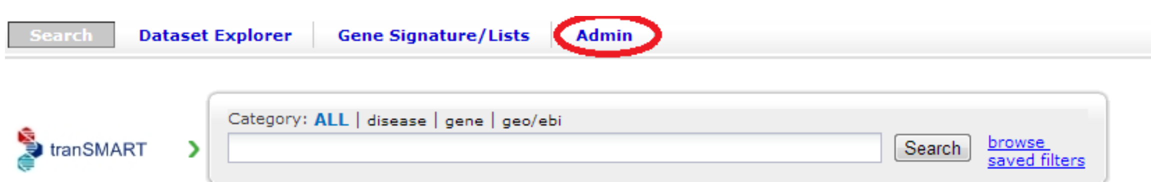
Administrator Privileges

In addition to performing administration tasks, you, as the tranSMART User Administrator, are a tranSMART super-user with access privileges to all tranSMART resources, including all Dataset Explorer studies and both public and private gene signatures. You also have access to the tranSMART access log.

tranSMART user administrators are assigned the role `ROLE_ADMIN`.

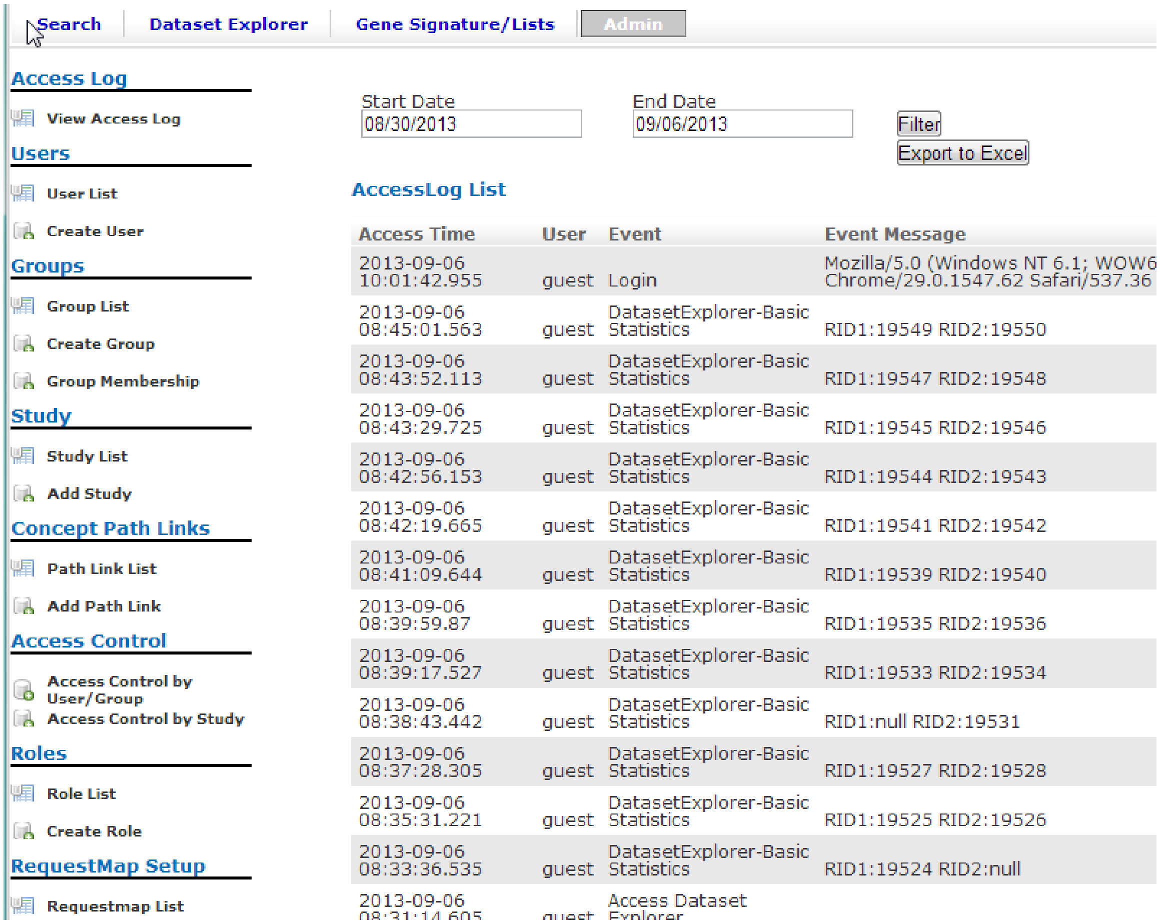
The Administrator's Console

To access the console where you perform administrator tasks, click the **Admin** tab:



Note: Only tranSMART users who are assigned the role `ROLE_ADMIN` can see the **Admin** tab.

On initialization, the administrator's console displays the tranSMART access log:



Tasks in the Administrator's Console

The tasks you can perform as administrator are listed vertically along the left edge of the administrator's console. The following table summarizes the tasks:

Administrator Task	Description
View Access Log	Display the tranSMART access log.
Group List	List all user groups, and edit or delete groups.
Create Group	Create a user group.
Group Membership	Add users to a group, or remove users from a group.
User List	List of all tranSMART users, and edit or delete users.
Create User	Create a tranSMART user.
Access Control by Group	Grant users and groups access privileges to private Dataset Explorer studies, or remove access privileges for users and groups.
Access Control by Study	Grant users and groups access privileges to private Dataset Explorer studies, or remove access privileges for users and groups.
Study List	List the Dataset Explorer studies that are protected by access control.
Add Study	Designate a Dataset Explorer study as a secure object – that is, one that is protected by access control.
Role List	List all tranSMART roles, and edit or delete roles.
Create Role	Create a tranSMART role.
Requestmap List	Display mappings between tranSMART roles and the tranSMART URLs that each role grants access to, and edit or delete mappings.
Requestmap Create	Create a mapping between a role and a tranSMART URL.

Chapter 2

Managing tranSMART Users

Managing users involves the following tasks:

- Creating and editing user accounts
- Assigning users roles
- Assigning users and groups access rights to private Dataset Explorer studies

Understanding User Roles and Access Rights

Users are granted permissions to access private Dataset Explorer studies in two ways:

- Through roles
- Through the access level assigned to the user or group for a private study

  For information about access levels, see Access Levels on page 27.

User Roles

When you create or edit a user account, you can assign the user one or more of the roles in the table below.

For information on creating or editing a user account, see Managing User Accounts on page 9.

Role	Permissions
ROLE_SPECTATOR	**tranSMART Search** ■ All functions **Dataset Explorer** ■ Access to a private study if the user is assigned a VIEW or EXPORT access level for the study. ■ Export ability for a private study if the user is assigned an EXPORT access level for the study. ■ Access to all studies in the Public Studies folder. No access level is required. **Note:** Users with this role cannot be assigned the OWN access level for a study. **Gene Signature** ■ Create signatures ■ View/clone/export public signatures
ROLE_STUDY_OWNER	**tranSMART Search** ■ All functions **Dataset Explorer** ■ Access to a private study if the user is assigned a VIEW, EXPORT, or OWN access level for the study. ■ Export ability for a private study if the user is assigned an EXPORT or OWN access level for the study. ■ Access to all studies in the Public Studies folder. No access level is required. **Gene Signature** ■ Create signatures ■ View/clone/export public signatures

Role	Permissions
ROLE_DATASET_EXPLORER_ADMIN	**tranSMART Search** ■ All functions **Dataset Explorer** ■ Access to all studies ■ Export ability for all studies **Gene Signature** ■ Create signatures ■ View/clone/export public signatures **Note:** The Dataset Explorer administrator has no user administration permissions.
ROLE_ADMIN	**tranSMART Search** ■ All functions **Dataset Explorer** ■ Access to all studies ■ Export ability for all studies **Gene Signature** ■ Create signatures ■ Perform all operations on public and private signatures **User Administration** ■ Full user administration functions
ROLE_PUBLIC_USER	This is a limited-access role used for trainee accounts and for non-Johnson & Johnson users on the training server. **tranSMART Search** ■ Search functions against public data only. All search results exclude internal Johnson & Johnson data such as clinical trials and documents. Also, the Pictor, ResNet, and GeneGo tabs are hidden, as are links to Ariadne Pathway Studio. **Dataset Explorer** ■ Access to studies in the Public Studies folder only. ■ Export ability for all public studies. **Gene Signature** ■ Create signatures ■ View/clone/export public signatures

Note: For information on creating new roles that you can assign to users, see User Roles on page 6.

Access Rights to Dataset Explorer Studies

Dataset Explorer studies can be either public or private. Public studies are in the **Public Studies** folder of the Dataset Explorer navigation tree. All other studies are private.

Access rights to public and private studies are as follows:

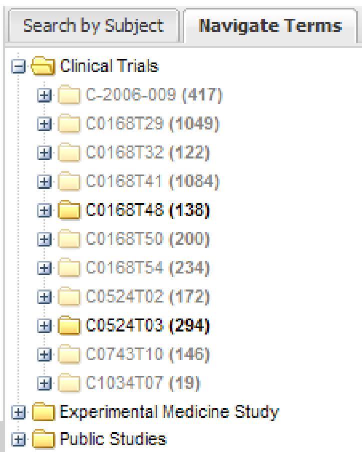
- Public studies

  All tranSMART users have full access to the studies in the Public Studies folder. No access level is required for these studies.

- Private studies

  By default, tranSMART users cannot access private studies. To allow a user to make comparisons between cohorts in a private study, you must grant the user access rights to that particular study.

If a user does not have access rights to a particular private study, the study is grayed out when the user displays the list of studies in the Dataset Explorer navigation tree. For example, in the following figure, the only private clinical studies the user has access to are C0168T48 and C0524T03:



> **Note:** Even if a user does not have access rights to a private study, the user can see a description of the study by right-clicking the study name in the navigation tree, and then clicking **Show Definition**.

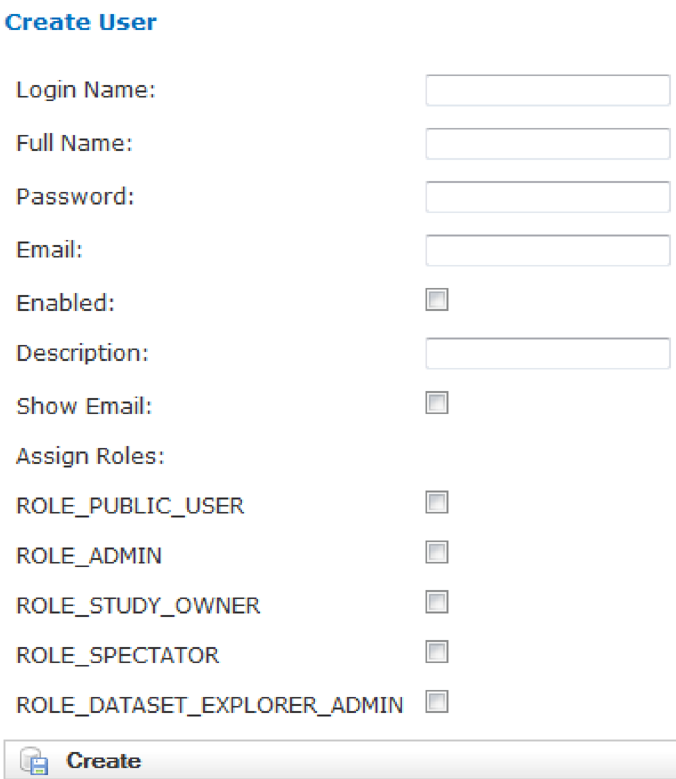
Managing User Accounts

Creating a User Account

To create a user account:

1. Click the **Admin** tab to display the administrator's console.
2. Click **Create User**.

   The Create User window appears:



3. Provide values for the fields in the Create AuthUser window, as follows:

Field	Description	Required
Login Name	The user's login ID.	Yes
Full Name	The name to display in the tranSMART window for this user.	Yes

Field	Description	Required
Password	This field is obsolete and will be removed in a future tranSMART release. Type any random text in this field. Do not give the user the text you type. Do not leave the field blank.	No
Email	The user's email address.	No
Enabled	Check this box to enable the user to log into tranSMART. If you leave the box blank, the user's account is disabled, and the user will not be able to log into tranSMART.	No
Description	An optional description of the user. The description appears in the user list (displayed with the **User List** task in the administrator's console).	No
Show Email	Check this box to display the user's email address. **Note:** The email display functionality is reserved for future use. Currently, the user's email address is displayed only when you or another User Administrator view or edit a user's account.	No
Assign Roles	Assign one or more roles to the user by checking the boxes next to the names of the roles to assign. If you do not check any of the boxes, the user will not be able to log into tranSMART. **Note:** For information about the roles you can assign to the user, see the section User Roles on page 6.	Yes

4. When finished defining the user account, click **Create**.

Editing or Deleting a User Account

To edit or delete a user account:

1. Click the **Admin** tab to display the administrator's console.
2. Click **User List**.

   The AuthUser List window appears.
3. Click the column heading **Full Name** to sort the list of user names alphabetically.

   Sorting the list may help you find the name in the list of users.

> **Note:** You can sort any of the columns in the AuthUser List by clicking the column heading.

4. Locate the name of the user whose account you want to edit or delete.
5. Click **Show** for the account to edit or delete:

WWID	Login Name	Full Name	Enabled	Description	
5123460	aanderson	Alan Anderson	true		Show
5123459	abrown	Agatha Brown	true		Show
5923951	achandler	Adam Chandler	true		Show

   The User window appears.

6. Take one of the following actions:
   - To delete the account, click **Delete**, then click **OK** to confirm the deletion.

     Note: Deleting a user account does not delete the user's records in the access log. Also, records of Dataset Explorer studies are independent of any associated user account. For example, if a user is the owner of a particular study, the study remains in Dataset Explorer even after the user is deleted, even if no other user has access privileges for the study.

   - To edit the account, click **Edit**. After making the edits, click **Update**.

Chapter 3

Managing tranSMART Roles

A role is mapped to one or more tranSMART URLs. Each URL provides access to a tranSMART resource.

If a user is assigned a particular role, the user is able to access the URL mapped to the role, and therefore, to the resource available through the URL.

For example, the role `ROLE_ADMIN` is mapped to the URL pattern `/authUser/**` on the tranSMART site. At this location, users assigned `ROLE_ADMIN` (that is, administrators like yourself) can view, create, edit, and delete tranSMART user accounts.

A URL pattern can be mapped to one or more roles. Since `/authUser/**` is mapped to no other role than `ROLE_ADMIN`, only users assigned this role can perform tasks on user accounts.

Understanding Role / URL Mappings

Roles are mapped to URLs on the Requestmap List window of the administrator's console:

Requestmap List

ID	URL Pattern	Roles	
1	/requestmap/**	ROLE_ADMIN	Show
2	/role/**	ROLE_ADMIN	Show
3	/authUser/**	ROLE_ADMIN	Show
5	/**	IS_AUTHENTICATED_REMEMBERED	Show
6	/login/**	IS_AUTHENTICATED_ANONYMOUSLY	Show
7	/css/**	IS_AUTHENTICATED_ANONYMOUSLY	Show
8	/js/**	IS_AUTHENTICATED_ANONYMOUSLY	Show
9	/images/**	IS_AUTHENTICATED_ANONYMOUSLY	Show
10	/search/loadAJAX**	IS_AUTHENTICATED_ANONYMOUSLY	Show
1753751	/accessLog/**	ROLE_ADMIN	Show
1753752	/authUserSecureAccess/**	ROLE_ADMIN	Show
1753753	/secureObject/**	ROLE_ADMIN	Show
1753754	/secureObjectPath/**	ROLE_ADMIN	Show

URLs in this window are expressed as fragments of URLs called URL patterns. tranSMART determines the full URL to associate with a role by adding the URL pattern to the root URL for the tranSMART site. For example, if the tranSMART root URL is `https://transmart.jnj.com/transmart` and the URL pattern is `/authUser/**`, the complete URL mapped to the role `ROLE_ADMIN` is the following:

```
https://transmart.jnj.com/transmart/authUser/**
```

The request map supports the ** pattern-matching characters. For example, in the above URL, the URL pattern `/authUser/**` matches both of the following URLs:

URL	Purpose
`https://hostname/transmart/authUser/list`	View, edit, and delete tranSMART users.
`https://hostname/transmart/authUser/create`	Create tranSMART users.

Default Role / URL Mappings

The following table describes the pre-defined mappings between tranSMART roles and URL patterns:

URL Pattern	Mapped Role	Purpose
`/accessLog/**`	`ROLE_ADMIN`	View the tranSMART access log. When you click the **Admin** tab to access the administrator's console, the log is displayed by default.
`/authUser/**`	`ROLE_ADMIN`	Create, view, edit, and delete tranSMART users. Currently, only tranSMART administrators can perform these tasks.
`/role/**`	`ROLE_ADMIN`	Create, view, edit, and delete tranSMART roles. Currently, only tranSMART administrators can perform these tasks.

<table>
<tr><th>URL Pattern</th><th>Mapped Role</th><th>Purpose</th></tr>
<tr><td>/requestmap/**</td><td>ROLE_ADMIN</td><td>Create, view, edit, and delete mappings between roles and URLs.

Currently, only tranSMART administrators can perform these tasks.</td></tr>
<tr><td>/authUserSecureAccess/**</td><td>ROLE_ADMIN</td><td>Create, view, edit, and delete a user’s access rights to specific clinical trials.</td></tr>
<tr><td>/secureObject/**</td><td>ROLE_ADMIN</td><td>Create, view, edit, and delete IDs and other attributes of a clinical trial.</td></tr>
<tr><td>/secureObjectPath/**</td><td>ROLE_ADMIN</td><td>No longer used.</td></tr>
<tr><td>/**</td><td>IS_AUTHENTICATED_REMEMBERED</td><td>Attempt to access any tranSMART URL.

Note that:
■ If the user has not yet logged into tranSMART, the tranSMART login screen appears.
■ If the user successfully logs in, or if the user is already logged in, access to the specified URL depends upon the user’s role.</td></tr>
<tr><td>/login/**</td><td>IS_AUTHENTICATED_ANONYMOUSLY</td><td rowspan="5">These URLs can be accessed by anyone.</td></tr>
<tr><td>/css/**</td><td>IS_AUTHENTICATED_ANONYMOUSLY</td></tr>
<tr><td>/js/**</td><td>IS_AUTHENTICATED_ANONYMOUSLY</td></tr>
<tr><td>/images/**</td><td>IS_AUTHENTICATED_ANONYMOUSLY</td></tr>
<tr><td>/search/loadAJAX**</td><td>IS_AUTHENTICATED_ANONYMOUSLY</td></tr>
</table>

Note: The roles IS_AUTHENTICATED_REMEMBERED and IS_AUTHENTICATED_ANONYMOUSLY cannot be edited, deleted, or explicitly assigned to users.

Managing User Roles

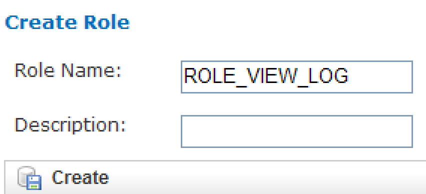
Creating a Role

To create a tranSMART user role:

1. Click the **Admin** tab to display the administrator's console.
2. Click **Create Role**.

   The Create Role window appears.
3. In **Role Name**, type a name for the role.

   Role names must be upper case and must be prefixed with ROLE_ – for example:



Note: In this example, a user assigned the role ROLE_VIEW_LOG can view the access log on the administrator's console, but cannot perform any of the other tasks on the console.

4. In **Description**, type a description for the role.

   A description is required.
5. Click **Create**.

   You must now map the role to a URL. Choose one of the following actions:

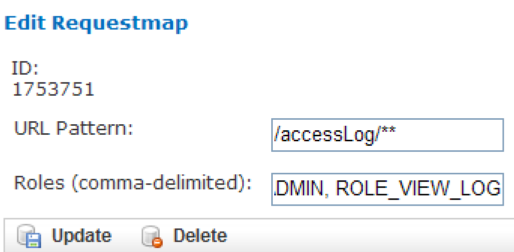
   - Adding a Role to an Existing Request Map (page 17)
   - Creating a New Request Map (page 17)

Adding a Role to an Existing Request Map

1. If the administrator's console isn't already displayed, click the **Admin** tab to display it.
2. Click **Requestmap List**.
3. Click **Show** for the mapping to which you want to add a new role:

9	/images/**	IS_AUTHENTICATED_ANONYMOUSLY	Show
10	/search/loadAJAX**	IS_AUTHENTICATED_ANONYMOUSLY	Show
1753751	/accessLog/**	ROLE_ADMIN	Show
1753752	/authUserSecureAccess/**	ROLE_ADMIN	Show
1753753	/secureObject/**	ROLE_ADMIN	Show

4. Click **Edit**.
5. In **Roles (comma-delimited),** type a comma and a space character after the rightmost role in the field, then type the name of the role to add to the map.



6. Click **Update**.

Creating a New Request Map

1. If the administrator's console isn't already displayed, click the **Admin** tab to display it.
2. Click **Requestmap Create**.
3. In **URL Pattern**, type the URL pattern to map to a role.

   Note: Double-check your entry to ensure that the URL exists. tranSMART does not validate the entry.

4. In **role (comma-delimited)**, type the role name in upper case.

   If you are mapping multiple roles to the URL, separate the role names with a comma.

5. Click **Create**.

Assigning a Role to a User

You assign a role to a user when you create or edit the user's account. For instructions, see Managing User Accounts on page 9.

Editing or Deleting a Role

To edit or delete a role:

1. If the administrator's console isn't already displayed, click the **Admin** tab to display it.
2. Click **Role List**.
3. Click **Show** for the role to edit or delete.
4. Take one of the following actions:
   - To delete the role, click **Delete**, then click **OK** to confirm the deletion.
   - To edit the role, click **Edit**. After making the edits, click **Update**.

Editing or Deleting a Request Map

To edit or delete a mapping between a role and a URL:

1. If the administrator's console isn't already displayed, click the **Admin** tab to display it.
2. Click **Requestmap List**.
3. Click **Show** for the map to edit or delete.
4. Take one of the following actions:
   - To delete the map, click **Delete**, then click **OK** to confirm the deletion.
   - To edit the map, click **Edit**. After making the edits, click **Update**.

Accessing the Administrator's Console

There are two ways for a user to attempt to access the administrator's console:

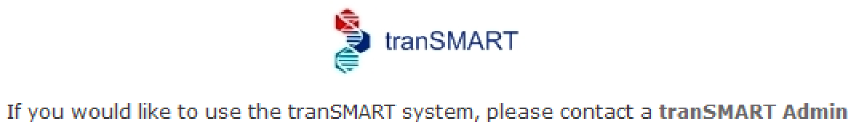
- Click the **Admin** tab on the tranSMART window (see The Administrator's Console on page 1).

  The **Admin** tab is displayed only for users who are assigned the role `ROLE_ADMIN`.
- Enter the complete URL for a task performed on the console.

For example, the following URL allows an administrator to create a new user:

`https://transmart.jnj.com/transmart/authUser/create`

A user who enters a URL for an administrative task, but who has not been assigned a role mapped to that URL, sees the following access-denied response:



Partial Administrator Rights

If a user is assigned a role that is mapped to one of the tasks on the administrator's console, that user can access the console and click on all of the links to administrator tasks. However, the only task the user will be allowed to perform is the one authorized through a role.

For example, suppose you create the role `ROLE_VIEW_LOG` to allow a user to view the tranSMART access log. A user with this role can view the log by entering the full URL for this administrator task – for example:

`https://transmart.jnj.com/transmart/accessLog/list`

However, if the user clicks on any of the other links on the administrator's console, the access-denied message is displayed.

Chapter 4

Managing Security for Dataset Explorer Studies

Users are able to perform operations with private Dataset Explorer studies only if you or another administrator grant the user (or a group that the user belongs to) access rights to do so.

Before you can assign a user or a user group access rights to a protected study, the following tasks must be performed:

1. The study must be loaded into a database server (Development, QA, Production).

   For information, see the tranSMART ETL Analyst's Guide.

2. You must protect the study by defining it as a secure object, using the tranSMART administrator's console.

   This step must be performed on the Development, QA, and Production servers separately, after the study has been loaded to the corresponding database server.

   The following section describes how to perform this task.

Managing Secure Objects

A secure object is a Dataset Explorer study that has restricted access. All studies except those in the Dataset Explorer Public Studies node should be defined as secure objects.

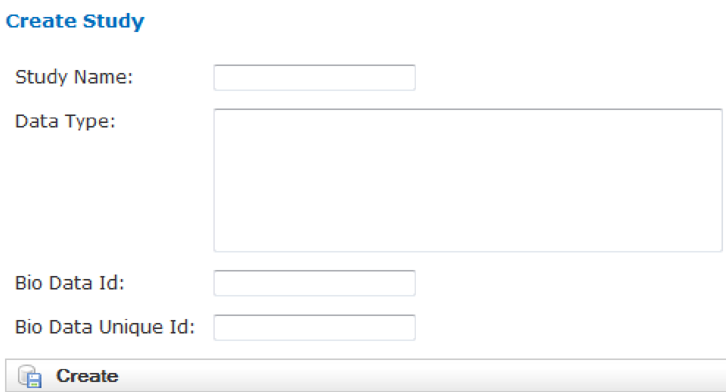
Defining a Secure Object

Note: To define a secure object in the administrator's console, you must have access to the information in the SEARCH_SECURE_OBJECT table (SEARCHAPP schema) for the study you are defining as a secure object.

To define a Dataset Explorer study as a secure object:

1. Click the **Admin** tab to display the administrator's console.
2. Click **Add Study**.

The Create SecureObject window appears:



Note that the fields in the Create SecureObject window correspond to columns in the SEARCH_SECURE_OBJECT table, as follows:

Create SecureObject Field	SEARCH_SECURE_OBJECT Column
Bio Data Id	BIO_DATA_ID
Data Type	DATA_TYPE
Bio Data Unique Id	BIO_DATA_UNIQUE_ID
Study Name	STUDY_NAME

3. Type the values from the SEARCH_SECURE_OBJECT table into the corresponding fields of the Create SecureObject window.
4. Click **Create**.

The Show SecureObject window appears, confirming the addition of the secure object.

Editing or Deleting a Secure Object

To edit or delete a secure object definition:

1. Click the **Admin** tab to display the administrator's console.
2. Click **Study List**.

   The SecureObject List window appears.

3. Click the ID of the secure object to edit or delete:

SecureObject List

Id	Bio Data Id	Data Type	Bio Data Unique Id	Display Name
263804	103	BIO_CLINICAL_TRIAL	EXP:C0168T48	Clinical Trial - C0168T48
263805	107	BIO_CLINICAL_TRIAL	EXP:C0524T03	Clinical Trial - C0524T03
263806	122	BIO_CLINICAL_TRIAL	EXP:C0743X01	Clinical Trial - C0743X01

4. Take one of the following actions:
   - To delete the secure object, click **Delete**, then click **OK** to confirm the deletion.
   - To edit the secure object, click **Edit**. After making the edits, click **Update**.

   Note: The Concept Paths field contains a link to SecureObjectPath. This path is no longer used and does not need to be defined.

Managing Groups

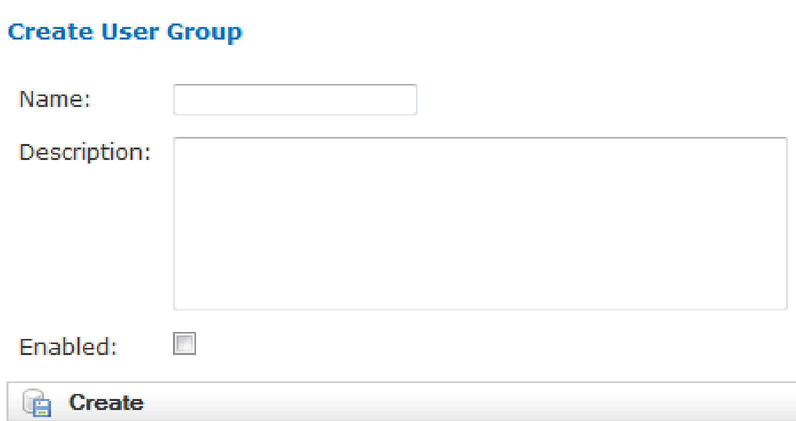
Access privileges for a study can be assigned to users individually or to a group of users. Assigning access privileges to a group of users can be more convenient than assigning privileges individually.

Creating a Group

To create a group:

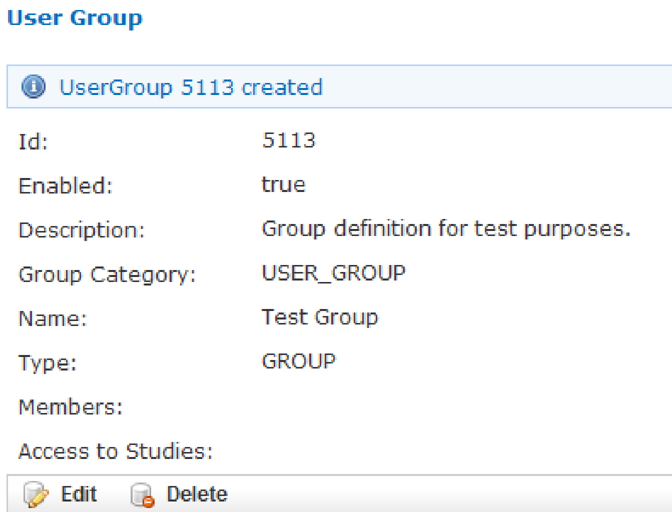
1. Click the **Admin** tab to display the administrator's console.
2. Click **Create Group**.

   The following window appears:



3. In **Name**, assign a name to the group.
4. Optionally, in **Description**, type an optional description of the group.
5. To enable the group's privileges, select **Enabled**.
6. Leave **Unique ID** blank. A unique ID will be assigned to the group.
7. Click **Create**.

In the following figure, the group Test Group has been created. Note that it currently has no members or privileges to access any studies.

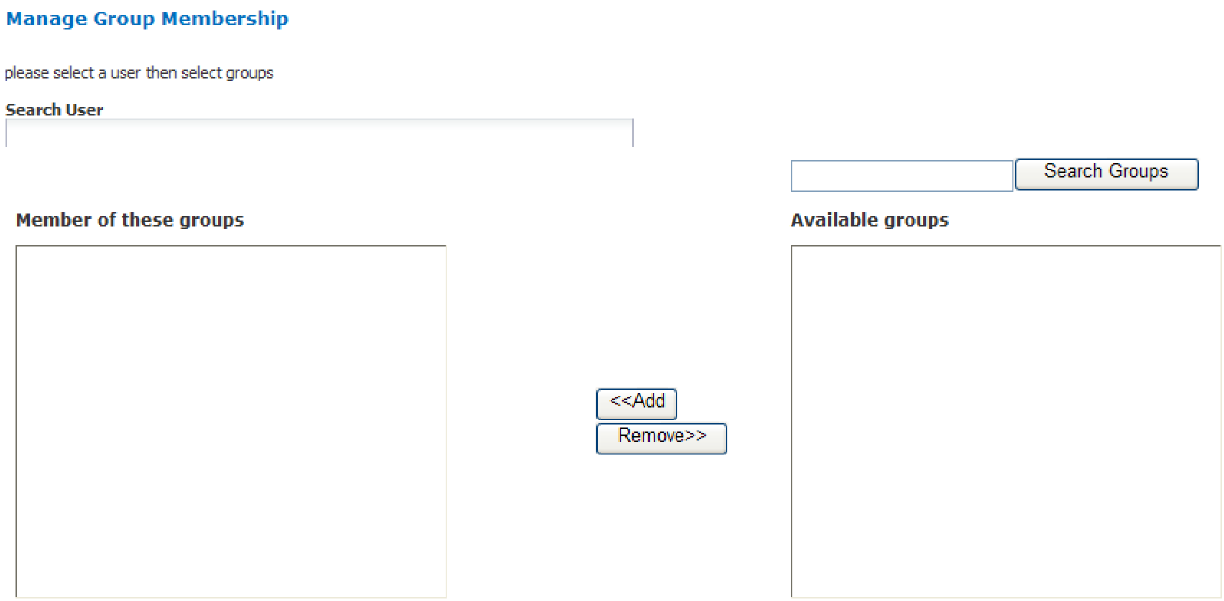


Managing a Group's Users

To add users to a group, or remove users from a group:

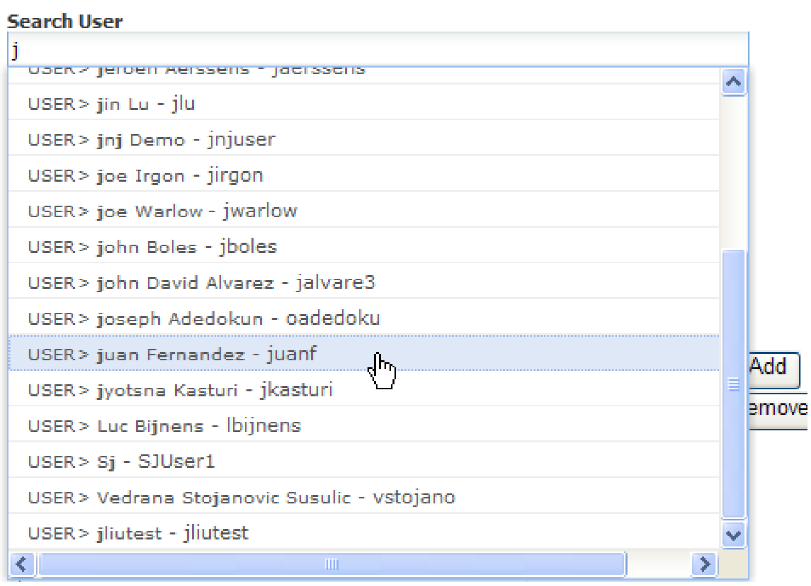
1. Click the **Admin** tab to display the administrator's console.
2. Click **Group Membership**.

The following window appears:



3. In **Search User**, type part or all of a user name, then select the name from the autotype dropdown.

   In the following figure, user Juan Fernandez is being selected:



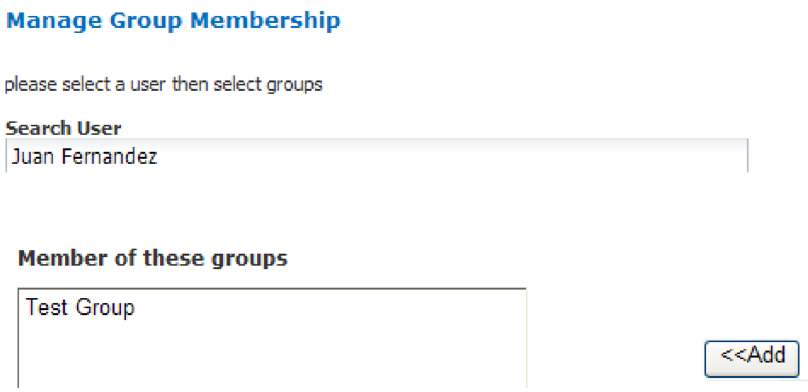
   Next you will specify the group that the user is being added to or removed from.

4. Click **Search Groups**.

   The list of the available groups appears in the **Available groups** box.

5. Click the group name, then click **Add** to add the user to the group, or **Remove** to remove the user from the group.

   In the figure below, the specified user has been added to the group Test Group:



6. Click another administrative task, or leave the administrator's console. No "Save" action is required.

Editing or Deleting a Group

1. Click the **Admin** tab to display the administrator's console.
2. Click **Group List**.
3. Click the ID of the group to edit or delete.
4. In the User Group window, click **Edit** or **Delete**:
   - If editing, make the changes and click **Update**.

     You may need to scroll down to the bottom of the window to see the edit fields.
   - If deleting, click **Delete**, then click **OK** to confirm the deletion.

Managing Access Privileges

You assign a user or group access privileges to a study by assigning the user or group a particular access level for the study. Access levels determine the kinds of operations that the user can perform when accessing the study.

Access Levels

Individual users and groups of users can be assigned the following access levels for a study:

Access Level	Description
OWN	User is the owner of the study with full access privileges.
EXPORT	User is not the owner of the study, but the user can define cohorts and points of comparison from the study. The user can also export all generated summary statistics and comparison data to a Microsoft Excel spreadsheet.
VIEW	User is not the owner of the study, but the user can define cohorts and points of comparison from the study. However, the user cannot export any data.

Managing Access Privileges for a User or Group

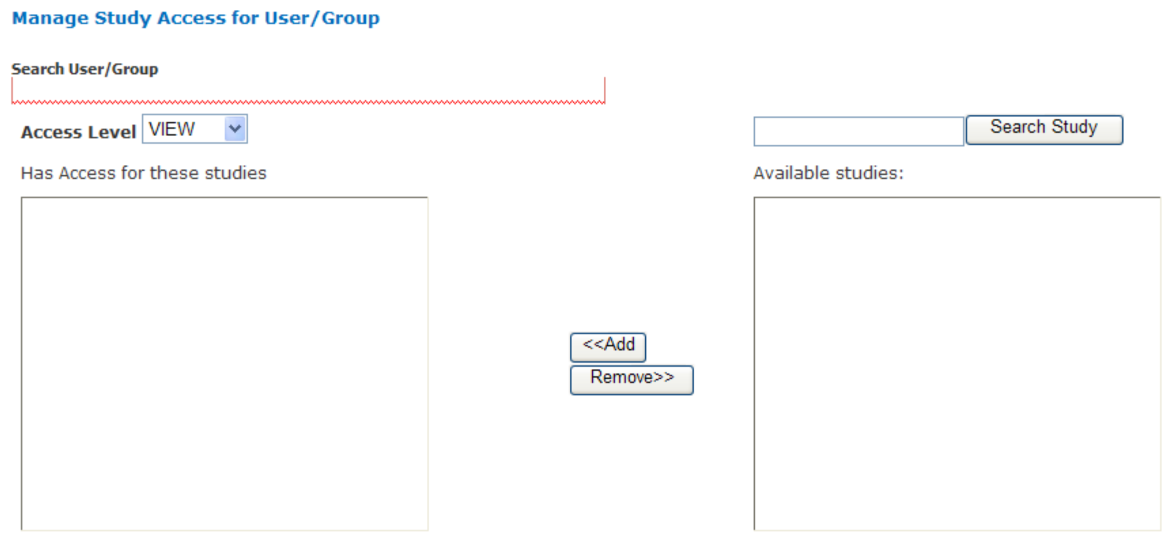
In the Manage Study Access for User/Group window, you can perform the following tasks:

- Assign or remove access privileges to one or more studies for a user or group.
- Assign the access level for the access privileges.

To assign a user or group access privileges for a study:

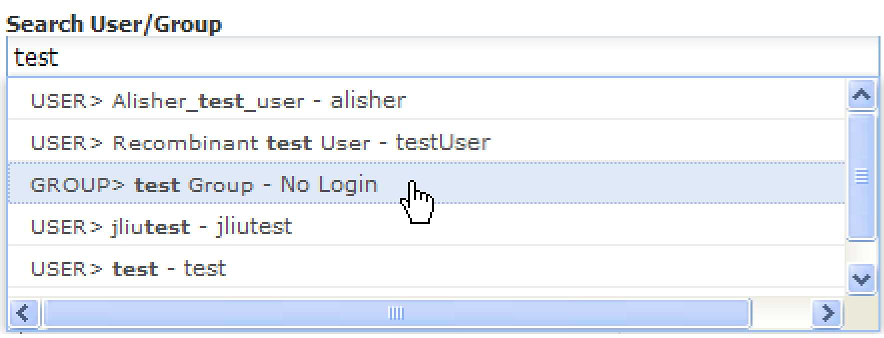
1. Click the **Admin** tab to display the administrator’s console.
2. Click **Access Control by User/Group**.

The following window appears:



3. In **Search User / Group**, type part or all of a user or group name, then select the name from the autotype dropdown.

   In the following figure, the group Test Group is being selected:



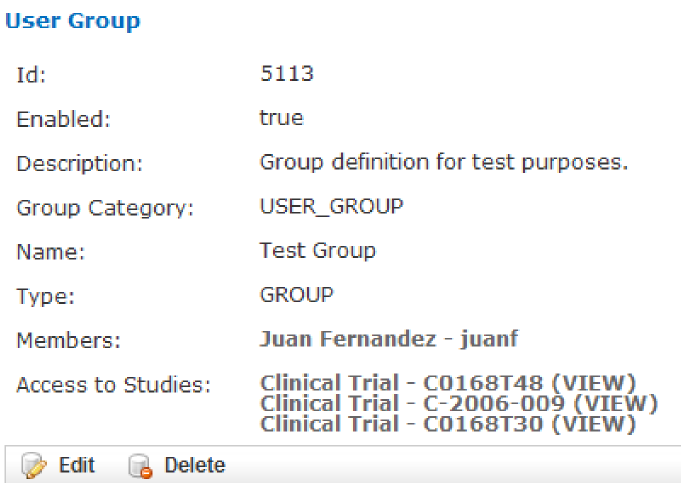
4. In the **Available studies** box, select one or more studies that the members of the group can access, then click **Add**.

5. In **Access Level**, select the access level (VIEW, EXPORT, OWN), to give to the members of the group for the selected studies.

   For descriptions of these access levels, see Access Levels on page 27.

6. Click another administrative task, or leave the administrator's console. No "Save" action is required.

If you now click **Groups > Group List**, and then click the ID of the new group you created in Creating a Group on page 23, you will see the members of the groups the studies to which the members have access privileges, and the access level for each study:



Managing Access Privileges for a Study

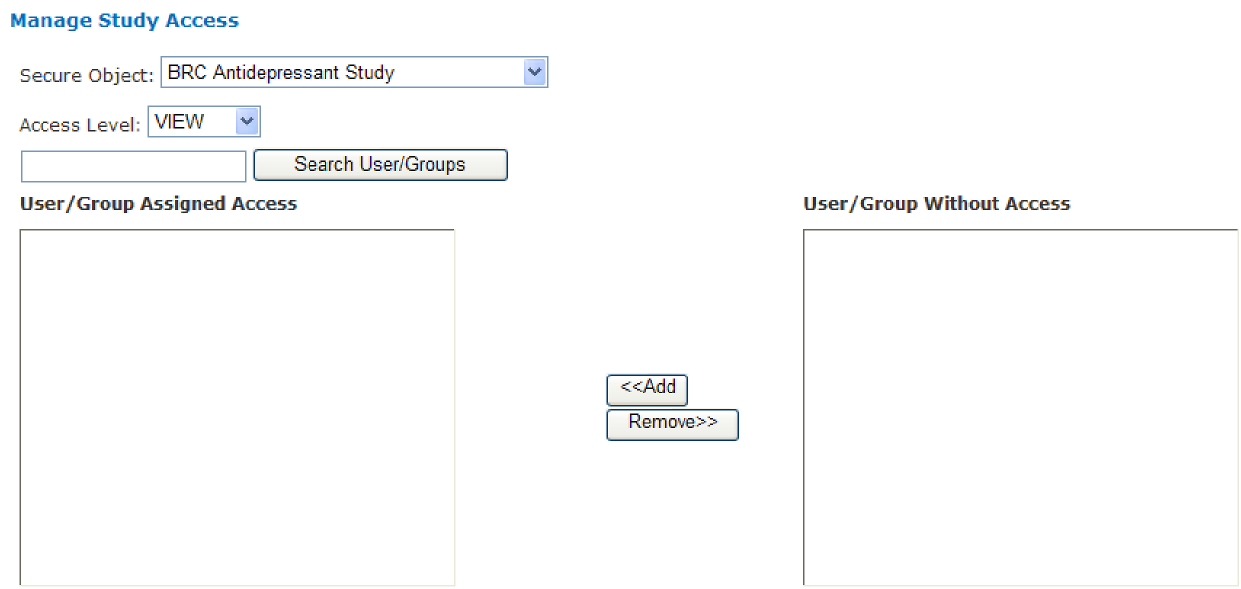
In the Manage Study Access window, you can perform the following tasks:

- Assign or remove access privileges to one or more users or groups for a secure object (such as a study or an entire study category).
- Assign the access level for the access privileges.

To grant access privileges to a study:

1. Click the **Admin** tab to display the administrator's console.
2. Click **Access Control by Study**.

The following window appears:



3. In **Secure Object**, select the study or study category to which access is being granted.
4. In the **User/Group Without Access** box, select the users and/or groups who can access the secure object, then click **Add**.
5. In **Access Level**, select the access level (VIEW, EXPORT, OWN) for accessing this secure object by the selected users/ groups.

   For descriptions of these access levels, see Access Levels on page 27.
6. Click another administrative task, or leave the administrator's console. No "Save" action is required.

Chapter 5

Viewing the tranSMART Access Log

The Access Log lets you view tranSMART events such as logins, logouts, searches, and Dataset Explorer analyses. For each event, the log notes the time and date of the event and the user who performed the operation.

The access log displays events beginning with the most recent.

The following figure shows an example of the access log.

Start Date 01/01/2009 End Date 09/11/2009 Filter Export to Excel

AccessLog List

Access Time	User	Event	Event Message
2009-09-11 10:05:16.807	trainee	Search	<SearchFilter.searchText:il4>
2009-09-11 09:39:02.626	trainee	Access Dataset Explorer	
2009-09-11 09:38:06.085	trainee	Login	Successful
2009-09-11 08:44:05.353	abrown	DatasetExplorer-Analysis by Concept	RID1:7292 RID2:7293 Concept:\\Clinical Trials\Clinical Trials\C0524T03\Subjects\Medical History\Atopy\Yes\
2009-09-11 08:44:05.345	abrown	DatasetExplorer-Grid Analysis Drag	RID1:7292 RID2:7293 Concept:\\Clinical Trials\Clinical Trials\C0524T03\Subjects\Medical History\Atopy\Yes\
2009-09-11 08:43:48.723	abrown	DatasetExplorer-Basic Statistics	RID1:7292 RID2:7293
2009-09-11 08:41:34.359	abrown	Access Dataset Explorer	
2009-09-11 08:41:31.377	abrown	Login	Successful
2009-09-11 08:40:31.572	abrown	Access Dataset Explorer	
2009-09-11 08:40:28.798	abrown	Login	Successful
2009-09-11 08:38:26.003	abrown	Access Dataset Explorer	
2009-09-11 08:38:20.078	abrown	Login	Successful
2009-09-11 08:37:38.867	abrown	Login	Successful
2009-09-11 07:49:37.758	trainee	Access Dataset Explorer	

Displaying the Access Log

When you open the administrator’s console, the log is displayed by default.

If you are in a different window of the administrator’s console and want to display the access log, click **View Access Log**.

Exporting the Access Log to a Spreadsheet

To export the access log to a Microsoft Excel spreadsheet:

1. With the access log displayed, click **Export to Excel**.
2. Specify whether you want to display the access log within a spreadsheet, or immediately save the spreadsheet to a file.

Specifying the Timeframe for the Access Log

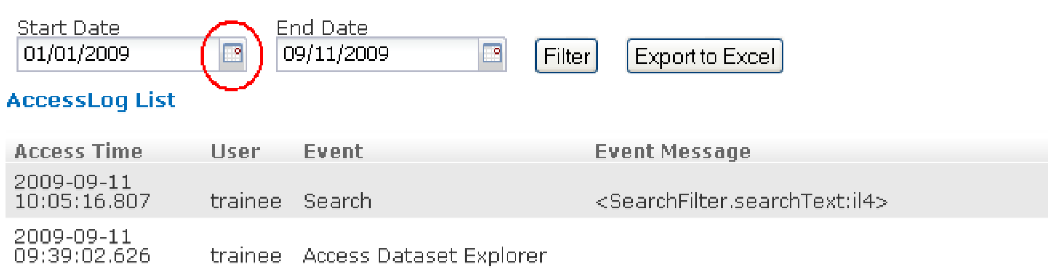
By default, the log shows all events, starting with the most recent event and extending back to the earliest.

You can specify a particular timeframe for the events you want to display or export.

To specify a timeframe:

1. With the access log displayed, type the date of the earliest events to display in the **Start Date** field.

   Alternatively, select the start date by clicking the calendar icon circled in red below, and then using the calendar controls to select the date:



2. Repeat Step 1 for the **End Date** field.
3. Click **Filter**.